REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-48 are pending in this application. Reconsideration is requested in view of the amendments and the remarks to follow.

Claims 20, 22, 29-31 and 37 have been amended responsive to minor informalities noted during review, however, these amendments are not intended to alter the scope of the claims. No new matter is added by the amendments to claims 20, 22, 29-31 and 37.

The amendments to the specification address minor informalities noted during review and/or bring the specification and drawings into mutual conformance. No new matter is added by the amendments to the specification.

35 U.S.C. §102

Claim 1 stands rejected under 35 U.S.C. §102(e) as being anticipated by Jain et al., U.S. Patent No. 6,047,325 (hereinafter "Jain"). Applicant respectfully submits that claim 1 is not anticipated by Jain and requests reconsideration in view of the discussion to follow.

Anticipation is a legal term of art. Applicant notes that in order to provide a valid finding of anticipation, several conditions must be met: (i) the reference must include every element of the claim within the four corners of the reference (see MPEP §2121); (ii) the elements must be set forth as they are recited in the claim (see MPEP §2131); (iii) the teachings of the reference cannot be modified (see MPEP §706.02, stating that "No question of obviousness is present" in conjunction with anticipation); and (iv) the reference must enable the invention as recited in the claim (see MPEP §2121.01). Additionally, (v) these conditions must be simultaneously satisfied.

Applicant notes the requirements of MPEP §2131, which states that "TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM." This MPEP section further states that "'A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.' *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). 'The identical invention must be shown in as complete detail as is contained in the ... claim.' *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an ipsissimis verbis test, i.e., identity of

terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)."

To clarify the legal meaning of the term "anticipation", Applicant notes the language of 35 U.S.C. §103(a):

> A patent may not be obtained though the invention is not **identically disclosed or described** as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This language sets forth Congressional intent in clear and exact terms as to what does or does not comprise anticipation, as compared to unpatentability. The reference must contain, within its four corners, **exactly** the subject matter of the claim, as it appears in the claim, in order to support a valid finding of anticipation.

In other words, 35 U.S.C. §102 is a rule of evidence pertaining to information in the public domain that *identically* discloses and enables the subject matter of a claim. As such, the *absence* of a claimed element in a reference is not a basis for *inferring* or *suggestion* of that claimed element in the context of anticipation.

The §102 rejection of claim 1 is believed to be in error. Specifically, the PTO and Federal Circuit provide that §102 anticipation requires that each and every element of the claimed invention be disclosed in a single prior art reference. *In re Spada*, 911 F.2d 705, 15 USPQ2d 1655 (Fed. Cir. 1990). The corollary of this rule is that the absence from a cited §102 reference of any claimed element negates the anticipation. *Kloster Speedsteel AB, et al. v. Crucible, Inc., et al.*, 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986).

No §103 rejection has been lodged regarding claim 1. Accordingly, if Applicant can demonstrate that Jain does not disclose any one claimed element with respect to claim 1, the §102 rejection must be withdrawn, and a subsequent non-final action made with a different rejection in the event that the Examiner still finds such claim to be not allowable.

In traversing the rejection, a brief review of the reference is helpful. Accordingly, such precedes the traverse of the respective anticipation rejection, as noted below.

Jain is directed to a: "Network device for supporting construction of virtual local area networks on arbitrary local and wide area computer networks" (Title). Jain teaches: "A network device that translates addresses of machines on physically separate networks and filters packets at the link, network and transport layers implements a virtual LAN over interconnected computer networks transparent to the computer networks. Using authentication and encryption, a secure connection between these network devices over a public wide area network implements a virtual private network and enables the definition of virtual LANs over the virtual private network. The network device has three tables for network address translation, routing, and filtering. *A controller processes each incoming packet* by translating network addresses to determine the destination of the packet, routing the packet to the determined location and filtering the packet according to filters defined for traffic between the source destination [sic] of the packet. If the packet is to be directed to a wide area network, encryption and authentication procedures can be provided to ensure secure transmission of the packet." (Abstract).

In contrast, claim 1 recites "A system comprising: a set of filters; a mapping of virtual addresses to network addresses; and a controller, coupled to the set of filters and the mapping, to, access, upon receipt of a data packet requested to be sent from a computing device to a target device via a network, the set of filters and determine whether the data packet can be sent to the target device based on whether the computing device is allowed to communicate with the target device, replace, based on the mapping, the target address in the data packet with a corresponding target network address; and forward the data packet to the target device at the target network address if it is determined the data packet can be sent to the target device", which is neither taught nor disclosed by Jain.

More specifically, Jain is silent regarding anything to "replace, based on the mapping, the target address in the data packet with a corresponding target network address", as recited in claim 1. Jain instead teaches (col. 4, line 13 et seq.; col. 4, line 40 et seq.) sending the MAC address to the originator of the packet, and teaches (col. 5, line 20 et seq.) maintaining both an IP address and a MAC address within the packet. As a result, Jain cannot possibly teach or disclose this affirmatively-recited aspect of the subject matter of claim 1.

Jain teaches (e.g., col. 4, line 10 et seq.) use of translation tables, however, translations may be disjunctive, e.g., substituting one description or language for another, in a fashion analogous to that of claim 1, or conjunctive, e.g., presentation of alternative descriptions or languages representative of the same underlying information, as in Jain, or, for that matter, and to use an example that should be familiar, a European patent (where the Detailed Description may be represented in three different languages in a single document).

Indeed, many common phrases used in English reflect the conjunctive sense - e.g., "null and void" employs an apparent redundancy, but the term "null" reflects middle French and Latin antecedents, while the term "void" reflects middle English and Latin antecedents, to establish notice such that parties speaking those different languages were, in forming a contract, able to readily extract the underlying notion of vacuity.

In even further contrast, the set of filters recited in claim 1 are defined (page 7, line 19 et seq.) to have a bidirectional capability. In other words, the set of filters is configured to be able to inspect incoming and/or outgoing data packets.

More specifically, Applicant's specification states that: "Filters 114 are a set of one or more filters that impose restrictions on the ability of the corresponding computing device to transmit data packets to and/or receive data packets from other computing devices. Upon receipt of a data packet, controller 112 accesses filters 114 to determine whether one or more of filters 114 indicate that the data packet cannot be sent to (if the corresponding computing device is attempting to send the data packet) the targeted device or received from (if the corresponding computing device is the targeted device of the data packet) the source device. If the data packet cannot be sent to the targeted device (or received from the source device), then controller 112 refuses to let the data packet through and drops the data packet. Alternatively, a message may be returned to the source of the data packet informing the source that it cannot send the desired packet."

As noted above, Jain explicitly teaches filtering of *incoming* data packets and does not provide any teaching of bidirectional filtering. Jain states (col. 4, line 1 et seq.) that:

> Network devices 26 and 28 enable the definition of virtual local area networks, in some cases over a virtual private network defined on a wide-area network. To perform this function, these devices have a structure such as shown in FIG. 4. The network device contains interfaces (60, 62 and 64) to each local area network to which it is connected. Any number of such interfaces may be provided. Similarly, an interface 66 connects the device to the wide area network. Any number of such interfaces may be calculated, including Ethernet, broadband and V.34 connections. A controller 68 processes packets received through the interface 60 according to information found in the address resolution protocol (ARP) table 70, routing table 72 and filter table 74. The ARP table 70 contains information that is used by the network device **to translate a received Internet protocol (IP) address 70a from an ARP request**, or other network layer address, into a corresponding media access control (MAC) address 70b, sometimes called a hardware address, that is returned to the sender of the ARP request to send a message to the designated IP address.

Jain does not even contemplate the issues addressed by Applicant for which remedies are encompassed within the ambit of Applicant's claim 1. As such, it is inconceivable that Jain could enable the subject matter embraced by claim 1.

Accordingly, (i) Jain does not provide the subject matter of claim 1, (ii) as it is expressed in claim 1, (iii) requires modification impermissible in attempting to establish anticipation and thus (iv) cannot enable the subject matter of claim 1 in the sense of 35 U.S.C. §112, 1ST ¶, as is required for anticipation. Failing all four of these criteria for anticipation also means that Jain cannot possibly meet them collectively. Jain thus fails all five of the conjunctive criteria noted above for a valid finding of anticipation. Accordingly, the anticipation rejection of claim 1 is prima facie defective and should be withdrawn, and claim 1 should be allowed.

Summary of Rejections under 35 U.S.C. §103:

Rejection I: Claims 2 and 3 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Audebert, U.S. Patent No. 6,694,436 (hereinafter "Audebert").

Rejection II: Claims 4, 39, 44 and 45 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden et al., U.S. Patent No. 6,717,949 (hereinafter "Boden").

Rejection III: Claims 5, 6, 28-32, 34-36 and 38, and apparently 37 (page 6, Office Action) stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss et al., U.S. Patent No. 6,141,749 (hereinafter "Coss") and further in view of Dennis et al., U.S. Patent No. 6,466,932 (hereinafter "Dennis") or Epstein III et al., U.S. Patent No. 6,684,335 (hereinafter "Epstein").

Rejection IV: Claims 7, 9 and 19-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert.

Rejection V: Claims 8 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and Boden et al., U.S. Patent No. 6,266,707 (hereinafter "Boden II").

Rejection VI: Claims 10-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and Audebert and further in view of Mayes et al., U.S. Patent No. 6,510,154 (hereinafter "Mayes").

Rejection VII: Claims 15 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and Audebert and further in view of Dennis or Epstein.

Rejection VIII: Claims 18 and 25-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and Audebert and further in view of Chopra et al., U.S. Patent No. 6,510,509 (hereinafter "Chopra").

Rejection IX: Claim 33 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss, Audebert, Dennis and/or Epstein and further in view of Chopra.

Rejection X: Claims 40 and 41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Taylor et al., U.S. Patent No. 6,728,885 (hereinafter "Taylor").

Rejection XI: Claims 42 and 48 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Coss and Audebert.

Rejection XII: Claim 43 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and Coss and further in view of Dennis and/or Epstein.

Rejection XIII: Claims 46 and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Audebert.

Applicant respectfully submits that claims 2-48 are not unpatentable over the cited references and requests reconsideration in view of the discussion to follow.

Applicant notes that Dennis issued on October 15, 2002 and was filed on March 16, 1999. The instant application was filed on October 24, 2000. Accordingly, Dennis would qualify as prior art only under the timing provisions of

35 U.S.C. §102(e). Dennis is assigned to the Microsoft Corporation (see cover sheet), as is the instant application.

Applicant notes the provisions of MPEP §706.02(l)(1), entitled "Rejections Under 35 U.S.C. 102(e)/103; 35 U.S.C. 103(c)". This MPEP section cites 35 U.S.C. §103(c):

> 35 U.S.C. 103. Conditions for patentability; non-obvious subject matter.
> (c) Subject matter developed by another person, which qualifies as prior art only under one or more of subsections (e), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

More specifically, this MPEP section states that "Effective November 29, 1999, subject matter which was prior art under former 35 U.S.C. 103 via 35 U.S.C. 102(e) is now disqualified as prior art against the claimed invention if that subject matter and the claimed invention "were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person." This change to 35 U.S.C. 103(c) applies to all utility, design and plant patent applications filed on or after November 29, 1999, including continuing applications filed under 37 CFR 1.53(b), continued prosecution application filed under 37 CFR 1.53(d), and reissues." Accordingly, Dennis is not available as prior art under 35 U.S.C. §103(a), and the rejections based on Dennis are thus moot.

Traverse I:

Claims 2 and 3 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Audebert. Portions of Jain are discussed hereinabove vis-a-vis claim 1, from which claims 2 and 3 depend.

Additionally, Jain teaches (col. 5, line 20 et seq.) that enhanced security follows from ensuring that both addresses are available to the sender. As such, Jain teaches away from the subject matter embraced by claims 2 and 3. It is improper to combine references where the references teach away from their combination. This is explained below in more detail with reference to MPEP §2145(X)(D), entitled "References Teach Away from the Invention or Render Prior Art Unsatisfactory for Intended Purpose". This MPEP subsection states that: "In addition to the material below, see MPEP §2141.02 (prior art must be considered in its entirety, including disclosures that teach away from the claims) and MPEP §2143.01 (proposed modification cannot render the prior art unsatisfactory for its intended purpose or change the principle of operation of a reference).

In a further subsection (2), entitled "References Cannot Be Combined Where Reference Teaches Away from Their Combination", this MPEP subsection states that: "It is improper to combine references where the references teach away from their combination. *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983)." Inasmuch as the intent of the proposed combination of Jain and Audebert is to arrive at the subject matter of claims 2 and 3, and Jain teaches away from that subject matter, the proposed modification of the teachings of Jain is improper.

Audebert is directed to a: "Terminal and system for performing secure electronic transactions" (Title). Audebert teaches that: "The terminal includes a terminal module (1) and a personal security device (31). The terminal module (1) is adapted to receive high-level requests from an application (Fap) installed on an electronic unit. The high-level requests are independent of the personal security device (31). The terminal module (1) and/or the personal security device (31) includes a reprogrammable memory for storing and a unit for executing a filter program (F) translating the high-level requests into at least one of either (i) at least one sequence of exchanges of data between the terminal module (1) and the user or (ii) a sequence of at least one elementary command that can be executed by the personal security device, together with a unit for protecting the filter program (F, 62) to prevent any modification of the filter program by an unauthorized entity. The filter program includes a unit for identifying and/or authenticating the source of requests sent by the application (Fap) installed in the electronic unit." (Abstract).

In contrast, claim 2 recites "A system as recited in claim 1, wherein the controller is further to prevent the computing device from modifying any of the filters in the set of filters", while claim 3 recites "A system as recited in claim 1, wherein the computing device includes the system", which recitations are not taught, disclosed, suggested or motivated by the cited references, alone or in any proper combination. As noted above, Jain teaches away from the subject matter embraced by claims 2 and 3.

The Office Action cites (page 3, item 7) col. 6, lines 46-61 and col. 12, lines 5-16 of Audebert for the proposition that such teaches one to "prevent modification the packet in a filter program." Applicant disagrees.

Col. 6, lines 46-61 states that:

> at least one of said terminal module and said personal security device comprises:
> at least one reprogrammable memory for storing at least one filter program translating said high-level requests into at least one of either (i) a sequence of at least one elementary command for being executed by said second software means of said second data processing means, or (ii) a sequence of data exchanges between said terminal module and said user via said second interface means, said data exchanges being executed by said first software means of said first data processing means, and
> means for protecting said filter software to prevent an unauthorised person reading and/or modifying said software, and
> at least one of said first and said second data processing means comprise a data processing device for executing said filter program.

This passage is silent as to whom the unauthorized parties might be. Col. 12, lines 5-16 states that:

> The object of the invention is to prevent a pirate from using the integrated circuit card of a user without their knowledge, for example by modifying the filter software controlling the card or the application software, or by loading a virus to bypass the application or the filter software. The embodiment described previously and its variants address these risks, by enabling verification of:
> the integrity of the filter software, and
> the source and the integrity of commands sent to the card via the reader 6, by authenticating them using a MAC, for example.

Neither of these passages teach, disclose, suggest nor motivate anything such that "the controller is further to prevent the computing device from modifying any of the filters in the set of filters", as recited in claim 2. In fact, the passage immediately preceding the latter passage states need for security, and that (col. 11, line 57 et seq.):

> Another method of verifying the integrity of the filter software is to have the second module signed by an authority guaranteeing the content of the filter software by means of a private key that is kept secret by the authority. The first loading module then, at the same time as performing the decrypting operation, performs a hashing operation on the second module and verifies the signature of this module using the public key associated with the private key of the authority.
> **The operations described above imply the use of keys on which the security of the application relies. These keys can be concealed** in the loading module, stored in the reader 6, or stored **on the integrated circuit card 31 itself**. Another possibility is to install the decryption and integrity verification module in the reader 6.

Audebert teaches that the user, and not an operator or system, should control the device, stating (Summary, col. 6, line 15 et seq.) that:

> The present invention aims to provide a terminal for carrying out secure electronic transactions of the type comprising a personal security device such as an integrated circuit card or other device fulfilling the same functions and a terminal module provided with means of interfacing the personal security device, such as an integrated circuit card reader, and **offering** by virtue of its software and/or hardware architecture and the security mechanisms that it includes **an enhanced level of security compatible with the fact that the terminal can be under the control of users** (*as opposed to terminals under the control of the operators*). (emphases added).

As such, the references cannot be properly combined, and, even if their teachings could somehow be combined, the references fail to provide the subject matter of the claims. Further, there is no guidance *within the references*, to assist the artisan in picking and choosing elements from the references to attempt to arrive at the claimed subject matter.

Accordingly, the rejection of claims 2 and 3 is in error and should be withdrawn, and claims 2 and 3 should be allowed.

Traverse II:

Claims 4, 39, 44 and 45 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden.

Boden is directed to a: "System and method for IP network address translation using selective masquerade" (Title). Boden teaches: "An address management system and method. ADDRESS statements and HIDE rule statements are processed to generate a file of masquerade rules for associating subsets of internal addresses among a plurality of public addresses. Responsive to these masquerade rules, network address translation is performed for incoming and outgoing IP datagrams. IP Network Address Translation (NAT) and IP Filtering functions provide firewall-type capability to a gateway system, such as the IBM AS/400 system. A customer's system administrator specifies specific NAT and Filtering rules (via the AS/400 Operational Navigator GUI). A type of NAT, called masquerade NAT, defines a many-to-one mapping in such a way as to allow the 'many' to specify subsets of IP addresses. This allows traffic separation, which improves throughput to and from external networks (e.g. the Internet), and also improves flexibility in IP address management." (Abstract).

In contradistinction, claim 4 recites "A system as recited in claim 1, wherein the controller is to make the computing device aware of the virtual addresses in the mapping but to hide the network addresses in the mapping from the computing device", claim 39 recites "A method comprising: maintaining an association of virtual addresses and corresponding network addresses; making a computing device aware of the virtual addresses; hiding the network addresses from the computing device; receiving, from the computing device, a data packet

intended for a target computing device corresponding to a target virtual address; replacing, based on the target virtual address, the target virtual address with the corresponding target network address; and forwarding the data packet to the target computing device at the target network address", claim 44 recites "One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 39" and claim 45 recites "A network mediator comprising: a mapping of virtual addresses to network addresses; and a controller, coupled to the mapping, to, make a corresponding computing device aware of the virtual addresses, hide the network addresses from the computing device, receive, from the computing device, a data packet intended for a target computing device corresponding to a target virtual address, replace, based on the target virtual address, the target virtual address with the corresponding target network address, and forward the data packet to the target computing device at the target network address", which recitations are not taught, disclosed, suggested or motivated by the cited references.

More specifically, Boden teaches (col. 4, line 29 et seq.) that "A key aspect of the invention lies in step 101 - the outbound datagram source IP address is compared to either a list of addresses, a subnet mask or a range of addresses. So, the broad result achieved is that, a) the internal (TRUSTED) addresses never appear in IP datagrams leaving the masquerade NAT system (which provides security and IP address isolation advantages), b) the many-to-one NAT means only a single public address is 'consumed' (a resource of increasing rarity) while allowing man [sic] internal systems to communicate to external system [sic], and

c) the entire process is completely invisible to external systems (no changes of configuration necessary other than to the NAT system)."

In contrast, Jain teaches (col. 5, line 20 et seq.) that "Additional security may be provided by binding machines to both the MAC and IP addresses and having filters that check both the MAC and IP address of a source of a message." Boden clearly teaches away from the teachings of Jain, and, further, the main intent of Boden, to ensure that the internal addresses NEVER leave the system in a datagram, is frustrated in adapting the teachings of Boden as taught by Jain. It is improper to employ a reference in a manner that renders it unsatisfactory for the intended purpose of the reference.

This is explained below in more detail with reference to MPEP §2143.01, entitled "Suggestion or Motivation to Modify the References". In a subsection entitled "THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE", this MPEP portion states that: "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)."

Accordingly, it is improper to attempt to combine the teachings of Jain and Boden to try to arrive at the subject matter of *any* of Applicant's claims. For at least these reasons, the rejection of claims 4, 39, 44 and 45 is inapposite and should be withdrawn, and claims 4, 39, 44 and 45 should be allowed.

Traverse III:

Claims 5, 6, 28-32, 34-36 and 38, and apparently 37 (page 6, Office Action) stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Dennis or Epstein. As noted above, Dennis is not available as prior art under 35 U.S.C. §103(a). As also noted above, Jain teaches away from the subject matter of claim 1, from which claims 5 and 6 depend.

Coss describes: "Methods and apparatus for a computer network firewall with stateful packet filtering" (Title). Coss teaches that: "The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." (Abstract).

In contrast, claim 5 recites that "the controller is further to allow the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels", while claim 6 recites "further comprising allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device", claim 28 recites "A method comprising: maintaining a set of filters that restrict the ability of a computing device to communicate with other computing devices; allowing multiple remote computing devices, each corresponding to a different managerial level, to modify the set of filters; and preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device" and claim 35 recites "One or more computer-readable media having stored thereon a computer program to implement a multiple-level filter administration scheme and including a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including: allowing a first computing device operating at a first of the multiple levels to modify a set of filters corresponding to a filtered device; and allowing a second computing device operating at a second of the multiple levels to modify the set of filters only if the modification is at least as restrictive as the filters imposed by the first computing device", which recitations are not taught, disclosed, suggested or motivated by the cited references, alone or in any proper combination.

The Office Action states (pp. 4, 5, item 12) that Jain does not disclose that "the controller is further to allow the set of filters to be modified by a plurality of

remote devices operating at a plurality of different managerial levels." and "However, Coss discloses remote proxy of administrator loads filters (Coss: column 9 lines 7-18)." The Office Action further states that "It would have been obvious to one having ordinary skill in the art to combine the teachings of Coss within the system of Jain because it is well known in the art." Applicant disagrees for a number of reasons, as is explained below in more detail (see also Discussion of Unpatentability, infra). Notably, even if the proposed combination were permissible, the result fails to provide a number of affirmatively-recited elements in Applicant's claims.

Coss describes (Summary; col. 9, line 17 et seq.) a number of dynamic rules in the context of a firewall. However, this discussion fails completely to address any plurality of managerial levels.

Further, Coss explicitly states (col. 1, line 25 et seq.) that: "Typically, a firewall administrator allows broad access which is consented to from one side of the firewall to the other, but blocks transmissions in the opposite direction which are not part of an active network session. For example, "inside" company employees may have unrestricted access through the firewall to an "outside" network such as the Internet, but access from the Internet is blocked unless it has been specifically authorized. In addition to such a firewall at a corporate boundary to the Internet, firewalls can be interposed between network domains, and can also be used within a domain to protect sub-domains. In each case, different security policies may be involved."

In contrast, the set of filters recited in claim 1 are defined (page 7, line 19 et seq.) to have a bidirectional capability. In other words, the set of filters is configured to be able to inspect incoming and/or outgoing data packets.

Applicant developed this system to overcome shortcomings of firewalls (see, e.g., Applicant's Background). Applicant is concerned with controlling access, based on knowledge of both the source and the target, and with precluding susceptibility to being bypassed (or otherwise attacked) by a user of the computer, for example, by erasing or disabling the firewall software, loading another operating system that can bypass the firewall, etc. (page 2, second full paragraph of Applicant's specification). The cited references do not even contemplate these issues and thus cannot teach, disclose, suggest or motivate the solutions, as recited in Applicant's claims.

Coss is concerned with limiting access to a computer or computer system from outside of the firewall, but is not concerned with restricting access to resources outside the system from within the system (see, e.g., col. 1, line 25 et seq.). Accordingly, the rules employed in the firewall taught by Coss are applied to packets that are coming from outside the firewall and are not applied to packets being transmitted from within the firewall. Combining the teachings of Coss with those from other references thus does not and cannot provide any "set of filters", as recited in Applicant's claims.

Epstein is directed to a: "Resistance cell architecture" (Title). Epstein teaches that: "A communication network implements a "resistance cell architecture." Each cell in the architecture comprises communication equipment such as a cell communication device coupled to one or more computers or

terminals. Each cell is only permitted to communicate directly with certain predetermined other cells in the architecture. If a cell has a communication to be transmitted to a cell to which it does not directly communicate, the communication will be sent from one cell to another until the communication reaches the intended recipient. A security breach in the network can quickly, easily and effectively be isolated using the resistance cell architecture. For example, once a security [sic] is detected, the cell through which the security intrusion is detected can be deactivated or destroyed thereby preventing communications from the infected cell or branch of the resistance cell architecture to reach other parts of the network. Various cells in the resistance cell architecture can act as master controlling cells of various other subordinate cells. Master cells control many functions and the communication behavior of their subordinate cells. A set of commands is made available to the administrators of the cells to initiate and configure the network. The commands includes [sic] a number of controls and sub-controls that permit the master cells to initiate subordinate cells into the resistance cell architecture, alter the operating characteristics of the architecture, and respond to detected security breaches and problems." (Abstract).

Epstein is notably void of the terms "firewall" and "filter". As such, it is inconceivable that Epstein could motivate or suggest combination of the disclosure of Epstein with that of the other references as the Office Action proposes.

Accordingly, the proposed combination fails to provide the claimed subject matter and is improper. The rejection of claims 5, 6, 28-32 and 34-38 is defective and should be withdrawn, and claims 5, 6, 28-32 and 34-38 should be allowed.

Traverse IV:

Claims 7, 9 and 19-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert.

Claim 7 recites "A method comprising: maintaining, at a computing device, a set of filters that restrict the ability of the computing device to communicate with other computing devices; allowing the set of filters to be modified from a remote device; and preventing the computing device from modifying the set of filters", claim 20 recites "A network mediator comprising: a set of filters; and a controller, coupled to the set of filters, to, access, upon receipt of a data packet requested to be sent from a computing device to a target device via a network, the set of filters and determine whether the data packet can be sent to the target device based on whether the computing device is allowed to communicate with the target device, and prevent the computing device from modifying any of the filters in the set of filters" which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (p. 7, item 19) that "Audebert discloses that preventing unauthorized modification of filter software (Audebert: column 6 lines 46-61 and column 12 lines 5-16)." Applicant disagrees.

Audebert teaches use of a relatively elaborate cryptographic approach to transactions such as electronic fund transfer schemes and smart cards. In other words, Audebert is directed to a different set of issues, and the main intent of Audebert is frustrated in attempting to combine the teachings of Audebert with those from Jain and Coss because these references fail to even contemplate the issues to which Audebert is directed. As such, there can be no guidance in the

references to inform or suggest to the artisan which elements to select or how to combine them.

Audebert teaches (col. 6, line 62 et seq.) that: "The invention defined hereinabove achieves the security objectives required for carrying out electronic transactions by virtue of the fact that it describes a filter or "firewall" between the external world, i.e. the applications themselves, and the security means and peripheral devices that it controls, by means of a logical interface defining the format of high-level requests issued by the applications and of a translation software for processing these requests." Audebert repeatedly states (col. 3, line 51 et seq.; col. 4, line 65 et seq.; col. 26, line 50) that protection of the user's confidential information from viruses and other tools of pirates is a primary objective. Such relies on one-way "firewall" protection as described hereinabove with respect to Jain and Coss.

Furthermore, the system taught by Audebert requires use of a secret parameter (col. 25, line 17 et seq.) in order to be useful for the purposes to which Audebert intends to employ such system. Incorporation of some portions of the teachings of Audebert, but not others, into the systems taught by Jain and/or Coss renders the teachings of Coss unsuitable for their intended purpose. It is improper to employ a reference in a manner that makes it unsuitable for its intended purpose (see §2143.01, supra). Furthermore, the lack of motivation in the references suggests use of an improper "obvious to try" standard (discussed infra) for attempting to find unpatentability.

Accordingly, the rejection of claims 7, 9 and 19-24 is defective and should be withdrawn, and claims 7, 9 and 19-24 should be allowed.

Traverse V:

Claims 8 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and Boden II.

Boden II is directed to a: "System and method for IP network address translation and IP filtering with dynamic address resolution" (Title). Boden II describes: "IP network address translation (NAT) and IP filtering with dynamic address resolution in an Internet gateway system. Symbolic interface names are recognized in selected rule statements. An [sic] symbolic s-rule file is generated from these rule statements which includes symbolic interface names. During processing of a packet message, the s-rule file corresponding to the interface name in the packet message is processed, with symbolic addresses in the s-rule file resolved to the IP addresses obtained from the packet message." (Abstract).

Claim 8 recites "restriction of the ability of the computing device to communicate with other computing devices comprises restricting the computing device from transmitting data packets to one or more other computing devices" while claim 17 recites that "each filter includes a plurality of filter parameters, and wherein each of the plurality of filter parameters can include wildcard values", which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (p. 9, item 25) that Boden II teaches, at col. 7, line 66 et seq., that each of the plurality of filter parameters can include wildcard values, as recited in claim 17. Applicant disagrees.

Boden II teaches (col. 7, line 66 et seq.) that "Some parameters of FILTER statement 230 allow a special value to be specified: "*"." Applicant notes that "some" is not "each" and is not equivalent thereto.

Boden II also teaches (col. 8, line 1 et seq.) that "For operational parameters such as DSTPORT 252, specifying "*" has the same effect as not providing the parameter; that is, the IP packet destination port is not checked. Boden II further states (col. 4, line 64 et seq.) that: "8. Where a '*' is allowed as a value, it used to specify 'any possible value' in statements such as SERVICE, FILTER, etc. **The only operand allowed to be used with '*' is '='.**" This is not equivalent to a wildcard substituting for a portion of a value.

As described in Applicant's specification at page 15, line 11 et seq., a "wildcard" is such that: "The parameters for fields 162 – 170 may also employ "wild cards", which allow **at least a portion of a parameter** to match anything." As such, it is possible to specify one portion of a parameter and to allow other portions to have any value. Simply ignoring a parameter, as taught by Boden II, is not equivalent to such.

For example, being able to set a telephone to not be able to call telephone numbers having a "900" prefix (e.g., using a mask comprising "900-***-****"), but allowing it to call numbers with an "800" prefix, might be a desirable capability. In the example given in Boden II, the address for the destination port is not checked when an asterisk is used in the corresponding filter statement. In other words, Boden II simply turns that filter segment off when such a symbol is present in the field. As a result, Boden II teaches a switch but does not teach,

disclose, suggest or motivate a wildcard. In fact, Boden II is void of the term "wildcard".

Accordingly, Boden II does not teach or disclose wildcard values as recited in Applicant's claims. As noted above with respect to Traverse IV, Jain fails to provide the elements for which Jain is cited, Audebert and/or Coss fails to cure the deficiencies of Jain and their teachings are not properly combinable. As a result, the rejection of claims 8 and 17 is prima facie defective and should be withdrawn, and claims 8 and 17 should be allowed.

Traverse VI:

Claims 10-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and Audebert and further in view of Mayes.

As noted above with respect to Traverse IV, Jain, Coss and/or Audebert fail to provide the elements for which they are cited, and their teachings cannot properly be combined as suggested in the Office Action. Mayes fails to cure these deficiencies.

Mayes is directed to a: "Security system for network address translation systems" (Title). Mayes teaches that: "A system and method are provided for translating local IP addresses to globally unique IP addresses. This allows local hosts in an enterprise network to share global IP addresses from a limited pool of such addresses available to the enterprise. The translation is accomplished by replacing the source address in headers on packets destined for the Internet and by replacing destination address in headers on packets entering the local enterprise network from the Internet. Packets arriving from the Internet are screened by an adaptive security algorithm. According to this algorithm, packets are dropped and logged unless they are deemed nonthreatening. DNS packets and certain types of ICMP packets are allowed to enter local network [sic]. In addition, FTP data packets are allowed to enter the local network, but only after it has been established that their destination on the local network initiated an FTP session." (Abstract).

Claim 10 recites that "one or more filters in the set of filters restrict one or more of the transmission of data packets of a particular type from the computing device and reception of data packets of a particular type at the computing device",

claim 11 recites that "one or more filters in the set of filters restrict one or more of the transmission of Internet Protocol (IP) data packets from the computing device and reception of IP data packets at the computing device based on one or more of: a source address, a destination IP address, a source port, a destination port, and a protocol", claim 12 recites that "one or more filters in the set of filters identifies that a data packet targeting a particular address can be transmitted from the computing device to the addressed device, and further identifies a new address that the particular address from the data packet is to be changed to prior to being communicated to the addressed device", claim 13 recites that "one of the filters in the set of filters is a permissive filter that indicates a data packet can be passed to its targeted destination device if the data packet parameters match corresponding parameters of the filter" and claim 14 recites that "one of the filters in the set of filters is an exclusionary filter that indicates a data packet cannot be passed to its targeted destination device if the data packet parameters match corresponding parameters of the filter", which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (p. 9, item 27) that "Jain as modified does not explicitly disclose wherein one or more filters in the set of filters restrict one or more of the transmission of data packets of a particular type from the computing device and reception of data packets of a particular type at the computing device. However, Mayes discloses that limitation (Mayes: abstract and column 1 line 9 and column 2 line 32)." Applicant disagrees with the rejection and with the characterization of what Mayes teaches.

Mayes teaches (col. 7, line 13 et seq.) that: "It should be apparent from the above discussion that there is essentially no security mechanism to block outbound packets. Most enterprises expect this behavior." As such, Mayes teaches away from any restriction of "transmission of data packets of a particular type from the computing device" as recited in claim 10, any restriction of "transmission of Internet Protocol (IP) data packets from the computing device" as recited in claim 11, or any filter that "identifies that a data packet targeting a particular address can be transmitted from the computing device to the addressed device" as recited in claim 12.

Accordingly, the rejection of claims 10-14 is defective and should be withdrawn, and claims 10-14 should be allowed.

Traverse VII:

Claims 15 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and Audebert and further in view of Dennis or Epstein. As noted above, Dennis is not available as prior art under 35 U.S.C. §103(a).

Claim 15 depends from claim 7 and recites that "allowing comprises allowing the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels" and claim 16 depends from claim 15 and recites "further comprising allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device", which recitations are not taught, disclosed, suggested or motivated by the cited references.

As noted above with respect to Traverse IV, attempting to combine the teachings of Jain, Coss and Audebert fails to provide the subject matter of claim 7. Epstein fails to cure the deficiencies of that combination. As noted above with respect to Traverse III, Epstein is void of the term "filter", and thus cannot possibly teach, disclose, suggest or motivate the subject matter of claim 15 or claim 16.

Accordingly, the rejection of claims 15 and 16 is prima facie defective and should be withdrawn, and claims 15 and 16 should be allowed.

Traverse VIII:

Claims 18 and 25-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and Audebert and further in view of Chopra. As noted above with respect to Traverse IV, Jain fails to provide the elements for which Jain is cited, Audebert and/or Coss fails to cure the deficiencies of Jain and their teachings are not properly combinable. Chopra fails to cure these deficiencies, as is described below in more detail.

Chopra is directed to a: "Method and apparatus for high-speed network rule processing" (Title). Chopra teaches that: "A high-speed rule processing apparatus is disclosed that may be used to implement a wide variety of rule processing tasks such as network address translation, firewall protection, quality of service, IP routing, and/or load balancing. The high-speed rule processor uses an array of compare engines that operate in parallel. Each compare engine includes memory for storing instructions and operands, an arithmetic-logic for performing comparisons, and control circuitry for interpreting the instructions and operands. The results from the array of compare engines is [sic] prioritized using a priority encoding system." (Abstract).

Claim 18 recites that "the set of filters restrict the ability of the computing device to communicate with other computing devices on a per-data packet basis, wherein each filter includes a plurality of filter parameters, and wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in a data packet for the data packet to satisfy the filter", claim 25 recites "each filter in the set of filters includes a plurality of filter parameters, and wherein each filter parameter includes a filter

value and a mask value indicating which portions of the filter value must match a corresponding parameter in the data packet for the data packet to satisfy the filter", claim 26 recites that "the controller is to allow the data packet to be forwarded to the target device if the data packet satisfies the filter" and claim 27 recites that "the controller is to prevent the data packet from being forwarded to the target device if the data packet satisfies the filter", which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (page 12, item 36) that: "Jain as modified does not explicitly disclose wherein the set of filters restrict the ability of the computing device to communicate with other computing devices on a per-data packet basis, wherein each filter includes a plurality of filter parameters, and wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in a data packet for the data packet to satisfy the filter. However, Chopra discloses that limitation (Chopra: column 4 lines 25-26)."

The cited portion of Chopra states that: "Firewall protection provides network security. To prevent unauthorized access, the Internet gateway 130 processes packets with a set of firewall security rules that screen out packets related to unauthorized actions. For example, if the servers 141 and 143 are only to be used for internal purposes then the Internet gateway 130 should screen out all packets originating from the global Internet 100 and destined for the internal servers 141 and 143." Such does not comprise any set of filter that restrict the ability of any computing device to communicate with other computing devices on

a per-data packet basis because such is silent regarding outgoing packets. It merely restricts incoming packets according to a set of rules.

Accordingly, the rejection of claims 18 and 25-27 is prima facie defective and should be withdrawn, and claims 18 and 25-27 should be allowed.

Traverse IX:

Claim 33 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss, Audebert, Dennis and/or Epstein and further in view of Chopra. As noted above, Dennis is not available as prior art under 35 U.S.C. §103(a).

As also noted above, with respect to Traverse IV, Jain fails to provide the elements for which Jain is cited, Audebert and/or Coss fails to cure the deficiencies of Jain and their teachings are not properly combinable.

Applicant notes that the Office Action is silent as to any teachings of Epstein relative to claim 33. Clarification of the rejection and statement of a basis for inclusion of the reference are respectfully requested. As noted above with respect to Traverse III, Epstein is notably void of the terms "firewall" and "filter". As such, it is inconceivable that Epstein could motivate or suggest combination of the disclosure of Epstein with that of the other references as the Office Action proposes.

As noted above with particularity vis-a-vis Traverse VIII, Chopra fails to provide any teaching or disclosure of any "set of filters" to "restrict the ability of the computing device to communicate with other computing devices on a per-data packet basis" as recited in claim 33.

Further, the proposed combination fails to teach, disclose, suggest or motivate such in combination with "wherein each filter includes a plurality of filter parameters, and wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a

corresponding parameter in a data packet for the data packet to satisfy the filter", as recited in claim 33.

Accordingly, the rejection of claim 33 is improper and should be withdrawn, and claim 33 should be allowed.

Traverse X:

Claims 40 and 41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Taylor. As noted above with respect to Traverse II, Jain in view of Boden fails to provide the subject matter recited in claim 39, from which claims 40 and 41 depend. Taylor fails to cure the deficiencies of Jain and Boden, as is described below in more detail.

Taylor is directed to a: "System and method for network access control using adaptive proxies" (Title). Taylor teaches: "A method, system and computer program for providing multilevel security to a computer network. The method comprises the step of receiving a first communication packet on at least one network interface port from an outside network. The method further includes the steps of filtering the first packet in one of at least two levels of security comprising a first level of security which examines the content information of the packet and a second level of security which examines the first packet excluding the content information of the packet. The system includes a first packet filter configured to filter its input packets by examining content information of its packets and a second packet filter configured to filter its input packets by examining the header information without examining the content information of its packets. The system further includes a third filter which is configured to forward a number of packets to one of the first and second filters, thereby providing security to the computer network. The computer program includes a first module located in an application layer, a second module located in a network layer, and a third module located in a kernel space and configured to examine a number of packets received by the

computer network from at least one outside network and to forward the number of packets to one of the first and second modules after examining the number of packets." (Abstract).

Claim 40 recites that "the replacing comprises performing the replacing transparent to the computing device" while claim 41 recites "receiving, from a source device, another data packet that is intended for the computing device, wherein the other data packet includes a network address of the source device; and replacing, based on the network address of the source device, the network address of the source device with a corresponding virtual address", which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (page 14, item 41) that: "Jain as modified does not explicitly disclose wherein the replacing comprises performing the replacing transparent to the computing device. However, Taylor discloses that limitation (Taylor: column 2 line 47 - column 3 line 9)". Applicant disagrees.

The cited portion of Taylor states that:

> Conventional firewalls include only one of a packet filter, an application proxy and a stateful inspection.
> A packet filter examines each incoming packet and decides what actions to take by checking against a table of access control rules. The packet filter, in its simpler embodiments, examines the header information of each incoming packet and makes pass/fail decisions based on their source and destination addresses. A weakness of such a firewall is that the content information of the packets is unknown to the firewall. More specifically, because packet filters perform their checking at the network access layer, there is no real knowledge of application level vulnerabilities. As a result, direct connections are allowed between a source and destination computers through firewall 101, exposing internal hosts 105, 107, 109 to direct attacks.
> An application proxy does not allow direct contact between a 'trusted' and 'untrusted' networks [sic]. Each of the packets passing through this type of firewall is examined at the application layer--meaning the application proxies understand the destination and

> contents of packets. Such a firewall, for example, distinguishes between "FTP Put" and "Get" commands. A typical application proxy includes a built-in proxy function also known as a transparency function. The transparency function replaces the IP address of a host on the internal protected network with its own IP address for all traffic passing through. The transparency function provides added security, because it hides the addresses of internal hosts. This makes it more difficult for hackers on the outside to target specific devices inside such a firewall. For this higher security, however, the application proxy requires large amounts of processing power and a corresponding loss of performance. (emphasis supplied).
>
> Taylor continues on to state that:
>
> Finally, a stateful packet filter examines packets without examining the packets as well as that of an application proxy. After a packet filter firewall or stateful inspection firewall has decided to allow a connection to be made, it allows data to travel directly between the networks without further inspection. Once a session is opened, the nature of the session can be changed without being detected. This allows for more speed, but also creates potential security risks as well. Again, making internal hosts 105, 107, 109 vulnerable to attacks from outside.
>
> Accordingly, there exists a need for a firewall method which makes it possible to dynamically select the best procedures from existing firewall methods to achieve the required level of security while meeting performance constraints.

As such, Taylor teaches away from the type of firewall systems described in the passage referred to in the Office Action. The Office Action further states (page 14, item 41) that "It is well known in the art to address translation [sic], which is transparent." As noted above with respect to the traverse of the anticipation rejection, translation need not comprise replacement of one piece of information with another, as recited in claims 40 and 41. Accordingly, the statement in the Office Action is non sequitur to the subject matter of these claims, as are the references (e.g., col. 5, line 35 et seq.) in Taylor to translation.

Further, Taylor teaches use of a proxy 211 (col. 4, line 25 et seq.) that is part of the operating system of the computing device, and that includes user-defined rules for packet filtering (see, e.g., Fig. 2, item 209; also cover sheet of Taylor). As such, Taylor does not teach or disclose "hiding the network addresses from the computing device", as recited in claim 39, from which claims 40 and 41 depend.

Claims 40 and 41 include the recitation of claim 39 as described in 35 U.S.C. §112, 4TH ¶, stating that: Subject to the following paragraph, a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. **A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.**" Not only does Taylor not teach or disclose such recitation, but Taylor instead teaches (col. 3, line 1 et seq.) hiding internal addresses from external computing resources (see passage emphasized above). As such, Taylor fails to cure the deficiencies of the proposed combination.

Accordingly, the rejection of claims 40 and 41 is erroneous and should be withdrawn, and claims 40 and 41 should be allowed.

Traverse XI:

Claims 42 and 48 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Coss and Audebert. As noted above with respect to Traverse II, Jain in view of Boden fails to provide the subject matter recited in claim 39, from which claim 42 depends, or claim 45, from which claim 48 depends. Coss and/or Audebert fail to cure the deficiencies of Jain and Boden, as is noted above with respect to Traverses III-IX and also as noted below in more detail.

Claim 42 recites "further comprising: maintaining, at the computing device, a set of filters that further restrict the ability of the computing device to communicate with other computing devices; allowing the set of filters to be modified from a remote device; and preventing the computing device from modifying the set of filters", while claim 48 recites "further comprising: a set of filters that further restrict the ability of the computing device to communicate with other computing devices; and wherein the controller is further to, allow the set of filters to be modified from a remote device, and prevent the computing device from modifying the set of filters", which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (page 14, item 43) that: "Jain as modified does not explicitly disclose allowing the set of filters to be modified from a remote device and preventing the computing device from modifying the set of filters. However, Coss discloses that limitation (Coss: column 9 lines 7-18)". Applicant disagrees.

As noted above with respect to at least Traverse III, Coss does not provide any description of filters as the term is defined in Applicant's specification. As

noted above with respect to Traverse I, the cited portions of Audebert fail to teach, disclose, suggest or motivate anything to prevent the computing device from modifying the set of filters, as recited in claims 42 and 48. As such, the proposed combination fails to provide the subject matter of these claims.

For at least these reasons, the rejection of claims 42 and 48 is prima facie defective and should be withdrawn, and claims 42 and 48 should be allowed.

Traverse XII:

Claim 43 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and Coss and further in view of Dennis and/or Epstein. As noted above, Dennis is not available as prior art under 35 U.S.C. §103(a).

As also noted above with respect to Traverse II, Jain in view of Boden fails to provide the subject matter of any of Applicant's claims. As noted in Traverses III-X, Coss fails to aid in curing these deficiencies. As further noted in Traverses IV, VII and IX, Epstein fails to cure the deficiencies of the variously-cited references. This is explained below in more detail.

Claim 43 recites "A method as recited in claim 39, further comprising: maintaining a set of filters that restrict the ability of the computing device to communicate with other computing devices; allowing multiple remote computing devices, each corresponding to a different managerial level, to modify the set of filters; and preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device", which is not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (page 15, item 45) that: "Jain as modified does not explicitly disclose allowing multiple remote computing devices, each corresponding to a preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher level managerial device. However, Coss discloses remote proxy or administrator loads filters (Coss: column 9 lines 7-18)." Applicant disagrees.

As noted above with respect to at least Traverse III, Coss does not provide any description of filters as the term is defined in Applicant's specification. As noted above with respect to at least Traverse III, Epstein is notably void of the terms "firewall" and "filter". As such, it is inconceivable that Epstein could motivate or suggest combination of the disclosure of Epstein with that of the other references as the Office Action proposes or that such combination could provide the subject matter of claim 43.

For at least these reasons, the rejection of claim 43 is improper and should be withdrawn, and claim 43 should be allowed.

Traverse XIII:

Claims 46 and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Audebert. As noted above with respect to Traverse II, Jain and Boden fail to provide the subject matter of any of Applicant's claims. Audebert fails to cure the deficiencies of Jain and Boden, as is explained below in more detail.

Claim 46 recites that "the network mediator is communicatively coupled to the computing device" and claim 47 recites that "the computing device includes the network mediator", which recitations are not taught, disclosed, suggested or motivated by the cited references.

The Office Action states (page 16, item 47) that: "Jain as modified does not explicitly disclose wherein the network device is communicatively coupled to the computing device. However, Audebert discloses that limitation (Audebert: column 6 lines 46-61 and column 12 lines 5-16)." Applicant disagrees.

As noted above with respect to Traverse I, col. 6, lines 46-61 states that:

> at least one of said terminal module and said personal security device comprises:
> at least one reprogrammable memory for storing at least one filter program translating said high-level requests into at least one of either (i) a sequence of at least one elementary command for being executed by said second software means of said second data processing means, or (ii) a sequence of data exchanges between said terminal module and said user via said second interface means, said data exchanges being executed by said first software means of said first data processing means, and
> means for protecting said filter software to prevent an unauthorised person reading and/or modifying said software, and
> at least one of said first and said second data processing means comprise a data processing device for executing said filter program.

This passage is silent as to whom the unauthorized parties might be. Col. 12, lines 5-16 states that:

> The object of the invention is to prevent a pirate from using the integrated circuit card of a user without their knowledge, for example by modifying the filter software controlling the card or the application software, or by loading a virus to bypass the application or the filter software. The embodiment described previously and its variants address these risks, by enabling verification of:
> the integrity of the filter software, and
> the source and the integrity of commands sent to the card via the reader 6, by authenticating them using a MAC, for example.

Neither of these passages teach, disclose, suggest nor motivate anything such that a network mediator is coupled to anything. In fact, Audebert is void of the term "mediator". As such, it is inconceivable that the proposed combination could provide the subject matter of claims 46 and 47.

For at least these reasons, the rejection of claims 46 and 47 is erroneous and should be withdrawn, and claims 46 and 47 should be allowed.

Unpatentability:

All of the unpatentability rejections (discussed hereinabove with respect to Traverses I through XIII) fail to meet the standards set forth in the MPEP for establishing a prima facie case of unpatentability. These are set forth in MPEP §2142, entitled "Legal Concept of Prima Facie Obviousness" (see also MPEP §706.02(j).).

This MPEP section states that "To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." The references fail to teach or disclose the elements recited in the claims. Accordingly, the references cannot provide motivation to modify their teachings to arrive at the invention as claimed, and the Examiner has identified no such teaching or disclosure in the references. As a result, the first prong of the test cannot be met.

MPEP §2142 further states that "Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations."

Inasmuch as the references fail to provide all of the features recited in Applicant's claims, as set forth with specificity in the above traverses, the third prong of the test is not met. As a result, there cannot be a reasonable expectation of success. As such, the second prong of the test cannot be met.

MPEP §2142 additionally states that "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be

found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)." This fourth criterion cannot be met because the references fail to teach or disclose the elements recited in the claims.

Accordingly, the unpatentability rejections fail all of the criteria for establishing a prima facie case of obviousness as set forth in the MPEP.

Inasmuch as there is no guidance within the references, and as there is no basis for the Examiner's contentions within the cited references, the only possible motivation for these contentions is hindsight reconstruction wherein the Examiner is utilizing Applicant's own disclosure to construct a reason for combining the cited references. The Examiner is reminded that hindsight reconstruction is not an appropriate basis for a §103 rejection. (*See, e.g., Interconnect Planning Corp. v. Feil*, 227 USPQ 543, 551 (Fed. Cir. 1985); *In re Mills*, 16 USPQ2d 1430 (Fed. Cir. 1990) (explaining that hindsight reconstruction is an improper basis for rejection of a claim).).

The impropriety of "obvious to try" as a standard for unpatentability is described in more detail below with reference to MPEP §2145(X)(B). This MPEP section states that:

> The admonition that 'obvious to try' is not the standard under §103 has been directed mainly at two kinds of error. In some cases, what would have been 'obvious to try' would have been to vary all parameters or try each of numerous possible choices until one possibly arrived at a successful result, where the prior art gave either no indication of which parameters were critical or no direction as to which of many possible choices is likely to be successful.... In others, what was 'obvious to try' was to explore a new technology or general approach that seemed to be a promising field of experimentation, where the prior art gave only general guidance as to the particular form of the claimed invention or how to achieve it.

In re O'Farrell, 853 F.2d 894, 903, 7 USPQ2d 1673, 1681 (Fed. Cir. 1988) (citations omitted).

No indication as to which parameters are critical and no direction as to which of many possible choices is likely to be successful has been identified in the references relied upon.

Further, Applicant notes that no evidence has been provided as to why it would be obvious to combine or modify the teachings of these references. Evidence of a suggestion to combine or modify may flow from the prior art references themselves, from the knowledge of one skilled in the art, or from the nature of the problem to be solved. However, this range of sources does not diminish the requirement for actual evidence. Further, the showing must be clear and particular. See *In re Dembiczak*, 175 F.3d 994, 998 (Fed. Cir. 1999).

Dependent claims 2-6, 8-19, 21-27, 29-34, 36-38, 40-44 and 46-48 are allowable as depending from an allowable base claim and for their own recited features which are neither shown nor suggested by the prior art. For at least these reasons, Applicant respectfully requests that the §103 rejections of claims 2-48 be withdrawn, and that claims 2-48 be allowed.

Conclusion

To recapitulate the several legal arguments relative to alleged unpatentability:

(i) the references teach away from one another and the claimed subject matter; (ii) the teachings of the references are rendered unsuitable for their intended purposes if modified to arrive at the claimed subject matter; (iii) the proposed combinations fail to provide the claimed subject matter; (iv) the rejections fail to meet the criteria for a prima facie showing of unpatentability set forth in the MPEP; (v) the rejections are based on impermissible hindsight; (vi) the rejections employ an improper "obvious to try" standard; and (vii) no proper evidence of suggestion to modify or combine has been provided.

Claims 1-48 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: Nov. 28, 2004

By: _____

Frederick M. Fliegel
Reg. No. 36,138
(509) 324-9256 x239